1. The following documents (D) cited in the International Search Report are mentioned in this examination report:

D1: US-B1-6 356 638 (HARDY DOUGLAS ALLAN ET AL) 12 March 2002 (2002-03-12)

D2: SCHNEIER B:"APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C" JOHN WILEY & SONS, 1996, XP002322926 NEW YORK, US ISBN: 0-471-11709-9

D3: LU W P ET AL:"SECURE COMMUNICATION IN INTERNET ENVIRONMENTS:A HIERARCHICAL KEY MANAGEMENT SCHEME FOR END-TO-END ENCRYPTION" IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE INC. NEW YORK, US, Vol. 37, No. 10, 1 October 1989 (1989-10-01), pages 1014-1023, XP000070200 ISSN: 0090-6778

D4: US-B1-6 584 562 (FIORI COSTANTINO) 24 June 2003 (2003-06-24)

D5: TANENBAUM A S: "COMPUTER NETWORKS, PASSAGE" COMPUTER NETWORKS, LONDON : PRENTICE-HALL INTERNATIONAL, GB, 1996, XP002322927 ISBN:0-13-394248-1

D6: US-A-5 778 071 (CAPUTO ET AL) 7 July 1998 (1998-07-07)

2. The present application does not fulfill the requirements of Article 2(2) PCT because the object of claims 33 - 3 is not based on an inventive step in the sense of Article 33 (3) PCT.

2.1 Document D1 discloses a system for encrypting telephone conversations between one or more terminals in a packet-oriented data network and one or more terminals in a analog fixed telephone network, with the packet-oriented network and the telephone network being connected to each other via a gateway computer, and with the encryption and the exchange of keys which precedes it being executed in accordance with the end-to-end-principle.

(Document D1 also mentions the fact that all terminals must have the necessary encryption hardware. see e.g. column 2, lines 50-63. This includes the possibility of the "intermediate connection" of a separately-provided security module. In case of doubt, see document D6, Abstract and Figure 3).

What is not explicitly disclosed by D1 is the use during the above end-to-end session of the algorithms and protocols usual in the packet-oriented network for encrypted data transport and for key exchange.

2.2 Document D2 is taken from a well-known reference work, of which the contents can be consulted by the person skilled in the art without any inventive step (cf. the PCT Guidelines, PCT/GL/ISPE 13.13). It describes the principle of end-to-end encryption between telecommunication terminals (pages 216-220). In this context it mentions (page 219) the required use of the same encryption algorithm in both terminals, as well as the necessity of negotiating a common cryptographic key between the terminals on the basis of a key exchange protocol supported by them.

It would thus be obvious to the person skilled in the art, in order to guarantee compatibility, to equip all potential terminals involved in said secured end-to-end sessions with hardware (or software) which can process the data to be transported in accordance with the algorithms and protocols usual in the packet-oriented data network.

It follows from this that the object of the independent claim is not based on any inventive step (Article 33(3) PCT).

2.3 The compatibility problems presented by setting up secure end-to-end connections are not only known to the person skilled in the art from document D2. See e.g. D3, pages 1014 and 1015 or D4, column 1, line 59 to column 2, line 13. The contents of these documents are also suitable for formulating similar objections in respect of the requirements of Article 33(3) PCT.

2.4 It should also be noted that the following features contained in the dependent claims are known to the person skilled in the art:

-Conducting telephone conversations between terminals in an IP data network and terminals in a telephone network (TDM);

-The transmission of data over ISDN telephone networks. See D5, pages 139-144 (this document is also a known reference work);

-The setting up of modem connections (via which a PPP connection runs) in order to transport IP data packets (D5, pages 229-232).